UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH Apple ID prpr212324@gmail.com Apple ID ziyla718@icloud.com Apple ID art.money@icloud.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	No. 2:23-mj-368-KFW

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT APPLICATION

I, Michael Gagnon, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Drug Enforcement Administration (DEA), United States Department of Justice, with federal law enforcement jurisdiction, and have been in this position since January 2012. I joined the DEA Portland, Maine, Resident Office in 2018. I was assigned to the Los Angeles Division from 2012 until I moved to Portland. Prior to attaining sworn status as a Special Agent, I was employed by DEA and received specialized training in narcotics trafficking investigations and related legal matters at the DEA Training Academy in Quantico, Virginia. Before joining DEA, I was employed by the Newton Police Department in Newton, New Hampshire, from June 2009 to January 2012. During my employment with the Newton Police Department, I was a certified Peace Officer in the State of New Hampshire. I have received law enforcement training through the Police Standards and Training Counsel.

2. In the course of my employment with DEA, I have received approximately 17 weeks of training at the DEA Academy in Quantico, Virginia about techniques used by major narcotics traffickers. I have specialized training involving the use, possession, packaging, manufacturing, sales, concealment, and transportation of various controlled substances, money laundering techniques, and conspiracy investigations.

3. During my employment with DEA, I have participated in narcotics investigations both as a case agent and in a supportive role. I have participated in the arrests of multiple drug traffickers and in interviewing informants and suspects concerning the methods and means of drug traffickers. I have also participated in countless static and mobile surveillance activities and assisted in the execution of multiple search warrants and arrest warrants. I have conducted investigations regarding these unlawful activities, violations of Sections 841(a)(1), 843(b), 846, 952(a), and 963 of Title 21 of the United States Code, and Sections 2, 1952, 1956, and 1957 of Title 18 of the United States Code. As a DEA agent, I primarily investigate large-scale narcotics traffickers and money laundering organizations.

4. Based on my training and experience as a DEA Special Agent and police officer, I have become familiar with the criminal activities of individuals involved in drug trafficking organizations, including drug manufacture and distribution, money laundering, and unlawful use/possession of firearms.

5. The facts in this affidavit come from observations and information obtained from other DEA agents, police officers, and witnesses.

6. Based on my training, experience, participation in the investigation described below, and the facts set forth in this affidavit, I submit there is probable cause

to believe that violations of 21 U.S.C. §§ 841(a)(1) (distribution of controlled substances), 21 U.S.C. §§ 843(b) (unlawful use of a communication facility), and 18 U.S.C. § 1959 (violent crimes in aid of racketeering) (the "TARGET OFFENSES ") have been committed and that evidence, fruits, and/or instrumentalities of such are likely to be found in the location to be searched.

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States…that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. I adopt and incorporate the affidavit of Task Force Officer Thomas Lapierre filed on August 31, 2023, in support of a search warrant for a DNA swab of Nathaniel Ashwood (attached as Exhibit 1). I also adopt and incorporate my affidavit filed on October 20, 2023, in support of a search warrant directed to Verizon Wireless (attached as Exhibit 2) and the affidavit of TFO Lapierre filed on November 22, 2023, in support of a search warrant for an Apple iPhone (attached as Exhibit 3).

9. I am aware, based upon my training and experience and my conversations with other law enforcement officers, that iCloud accounts often contain substantial amounts of data that prove to be valuable evidence in proving violations of federal law. This evidence includes photos, videos, documents, and communications.

10. As described in Exhibit 2, I believe the following about telephone usage in the summer and fall of 2023:

a. Marcus Matthes utilized telephone number (267) 304-7715 ("Target Telephone 1" or "TT1");

b. Lloyd Lyttle utilized telephone number (207) 240-9812 ("Target Telephone 2" or "TT2").

11. Agents obtained a search warrant for a cellular telephone believed to be used by Nathaniel Ashwood. A search of this device revealed it is assigned telephone number (207) 631-6710 ("Target Telephone 3" or "TT3"). The search further revealed that the phone is assigned IMEI number 357197854034942 and linked to the iCloud account art.money@icloud.com.

12. According to records received from Apple, I learned the following about linked iCloud accounts:

a. The Apple ID prpr212324@gmail.com shows TT1 as the FaceTime/iMessage Phone and the verified phone number associated with the account. The subscriber is listed as "Poppy Roll." This Apple ID was created on October 8, 2019. This account is enabled for iCloud back up, calendars, iCloud photos, contacts, find my friends, iCloud drive, mail, messages in iCloud, notes, and sign in history.

b. The Apple ID ziyla718@icloud.com lists the verified phone number as TT2. The subscriber is "Yo Yo." This Apple ID was created on October 15, 2021. This account is enabled for linking calendars, iCloud photos, contacts, find my friends, iCloud drive, mail, notes, and sign in history.[1]

[1] This Court issued a search warrant directed to Verizon Wireless for information stored on Verizon's servers related to TT2. Verizon responded with very little text message data, which I believe either means

c. The phone assigned IMEI number 357197854034942 ("TT3") is linked to Apple ID art.money@icloud.com;[2]

BACKGROUND CONCERNING APPLE

13. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

15. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

16. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

17. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on

---

the data was not retained or the user of TT2 uses other platforms to communicate. Based upon the back-up settings, I believe it is likely that other information not recovered from Verizon Wireless is likely to be stored in the linked iCloud account.

[2] This Court issued a search warrant for the physical device. The review of the phone data is ongoing. I believe it is also likely that additional information is stored in user's iCloud account.

any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

18. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

19. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

20. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

21. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

22. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

23. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In

addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

24. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

25. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC

address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

26. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

27. In this case, I am seeking stored messages, photos, contacts, lists, and other data that is evidence of the crimes under investigation. In my training and

experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

28. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

29. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and

chronological context of access, use, and events relating to the crime under investigation.

30. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

31. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

32. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

33. Based on the forgoing, I request that the Court issue the proposed search warrant.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Michael Gagnon
Special Agent, DEA

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: Dec 12 2023

City and state: Portland, Maine

Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title